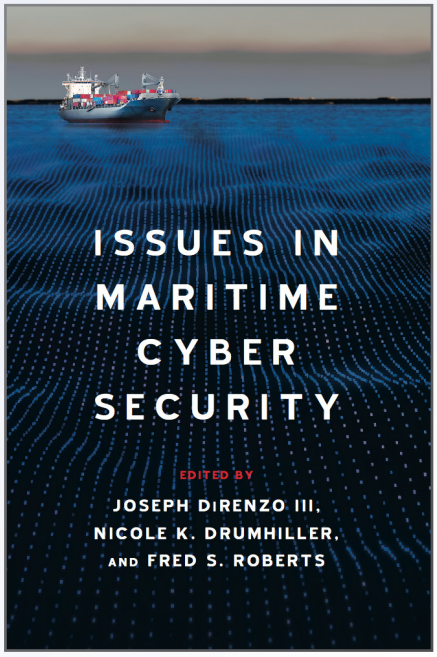
ISSUES IN MARITIME CYBER SECURITY

Editors: Dr. Joe DiRenzo III, Dr. Nicole K. Drumhiller, Dr. Fred S. Roberts

The world relies on maritime commerce to move exceptionally large portions of goods, services, and people. Collectively this effort comprises the Maritime Transportation System or MTS. A major component of this daunting multifaceted enterprise are cyber networks, and the infrastructure they control. From the complex programs managing the loading and unloading of containers to waiting trucks, to the global navigation systems onboard vessels, to the hydraulic valves designed to protect spills into waterways that are located and controlled by cyber systems within chemical, water/wastewater, or petroleum plants, the MTS is becoming increasingly automated.

The impact of the cyber element on the international MTS is significant. Yet, with the clear advantages this brings, come vulnerabilities, and challenges. Researchers have demonstrated that it is possible to remotely take control of a vessel by spoofing its GPS. The news has reported attacks that shut down a floating oil rig by tilting it. The electronic positioning software systems on ships are vulnerable to attacks that could modify files and charts, causing potential for serious damage. The complexity of the problem of making our MTS safe from cyber attack is daunting and the need for all stakeholders in both government (at all levels) and private industry to be involved in cyber security is more significant than ever as the use of the MTS continues to grow.

While there is literature about the maritime transportation system, and about cyber security, to date there is very little literature on this converging area. This pioneering book is beneficial to a variety of audiences, as a text book in courses looking at risk analysis, national security, cyber threats, or maritime policy; as a source of research problems ranging from the technical area to policy; and for practitioners in government and the private sector interested in a clear explanation of the array of cyber risks and potential cyber-defense issues impacting the maritime community.



About the Editors: Dr. Joe DiRenzo III is a retired Coast Guard Officer. Dr. Nicole K. Drumhiller is the Program Director of Intelligence Studies at American Military University. Dr. Fred S. Roberts is Director of the Department of Homeland Security University Center of Excellence CCICADA, based at Rutgers University.

COMING JULY 2017
WESTPHALIA PRESS

CHAPTER 1:
THREATS TO GLOBAL NAVIGATION

David B. Moskoff
U.S. Merchant Marine Academy

William G. Kaag
U.S. Navy (Ret.)

Abstract

This paper examines vulnerabilities of Global Navigation Satellite Systems (GNSS) and threats posed to these systems. Also considered are differences between maritime cyber threat issues such as radio frequency (RF) signal denial compared with traditional cyber threats. Various options available to the maritime community to mitigate these threats are discussed, such as crew training, stakeholder education, improved maritime equipment, and technological advances, including eLoran.

If this event had been a GPS failure instead of a GLONASS failure ... the entire world would have plunged into a catastrophe.

—Nunzio Gambale, CEO of Locata, after the 11-hour outage of GLONASS April 2014

Introduction

Originally developed to guide Allied convoys safely across the Atlantic, the use of synchronized low frequency radio signals as a navigational aid revolutionized modern maritime navigation in the 1940s. Faced with operating ships and aircraft over vast areas, researchers pioneered the use of radio signals to aid navigation in regions where poor weather conditions made traditional methods—

such as dead reckoning and celestial navigation—exceptionally difficult. This system was eventually named LOng RAnge Navigation (LORAN). When in range of three or more shore-based transmitters, LORAN receivers placed onboard ships and aircraft allowed operators to fix their location within minutes regardless of the weather. The original system, known as LORAN-A, and its eventual replacement, LORAN-C, were operated by the U.S. Coast Guard and other nations until 2010. The U.S. portions of the system were phased out in favor of the satellite-based Global Positioning System (GPS) which became operational in July of 1995. Figure 1 shows basic GNSS operation including GPS. The latest LORAN Position Navigation and Timing (PNT) system known as "eLoran" is currently in use or under consideration in several countries. Among the entities that historically operated and maintained these terrestrial loran systems are national Coast Guards or defense organizations. Eventually, Loran C systems throughout the world are expected to be replaced by eLoran or a similar complementary system.

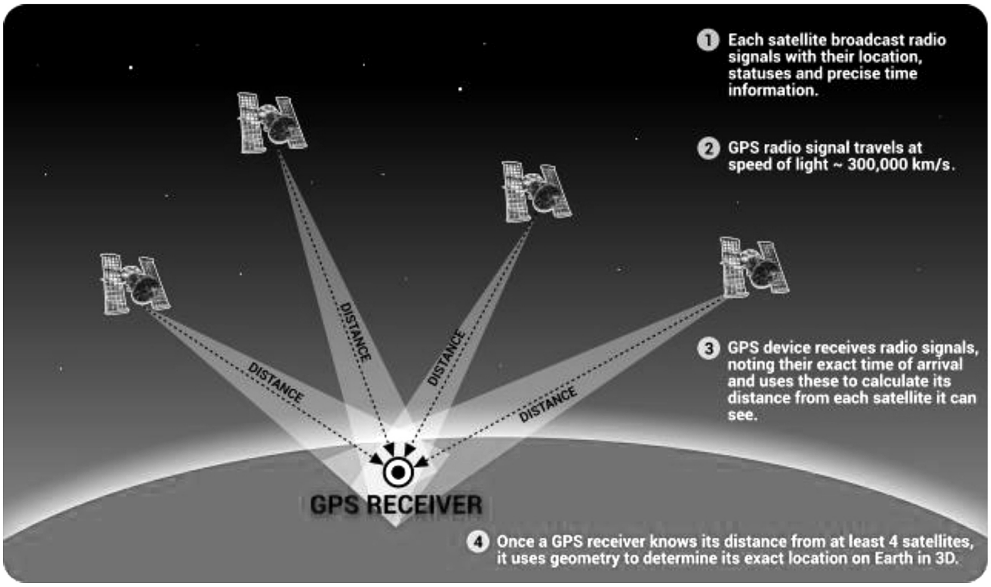


Figure 1: How satellite-based PNT systems operate—GPS as an example. (image courtesy of itsabouttimebook.com 2016 at http://itsabouttimebook.com/how-gps-works/time)

The impact of GPS on the commercial transportation industry has been enormous. Everything that moves—ships, cars, trains, aircraft, and even farm equipment—is now navigated by GPS, or a similar GNSS system. "Companies worldwide use GPS to timestamp business transactions, maintain records, and ensure traceability. Major financial institutions use GPS to" synchronize their computer networks around the world (National Coordination Office for Space-Based Positioning, Navigation, and Timing 2014). Large and small

businesses now use "automated systems that can track, update, and manage multiple transactions made by a global network of customers" (National Coordination Office for Space-Based Positioning, Navigation, and Timing 2014). These systems require accurate timing information often to nanosecond levels available through GNSS such as GPS (National Coordination Office for Space-Based Positioning, Navigation, and Timing 2014).

Reliance of the Maritime Industry on GNSS

The commercial maritime industry has become especially reliant on GNSS technology. The paper chart, which has been used on the bridge of most ships in one form or another for the past several hundred years, is being rapidly replaced by electronic charts—also called eCharts. eCharts provide a continuous, real-time plot of the true and relative movements of both the vessel and nearby objects often using radar images and automatic information system (AIS) transponder signatures superimposed on the electronic chart. Figure 2 is an example of a nautical eChart. Most merchant marine academies continue to teach their cadets skillsets such as how to fix a vessel's position using terrestrial and celestial bearings. However, these techniques are less often used in the modern shipping industry, which continues to move irreversibly toward the use of fully integrated electronic bridges.[1] Yet, in the event of GNSS compromise, these basic seamanship skills may be necessary to counter a cyber attack to provide the resiliency necessary to this vital transportation system.

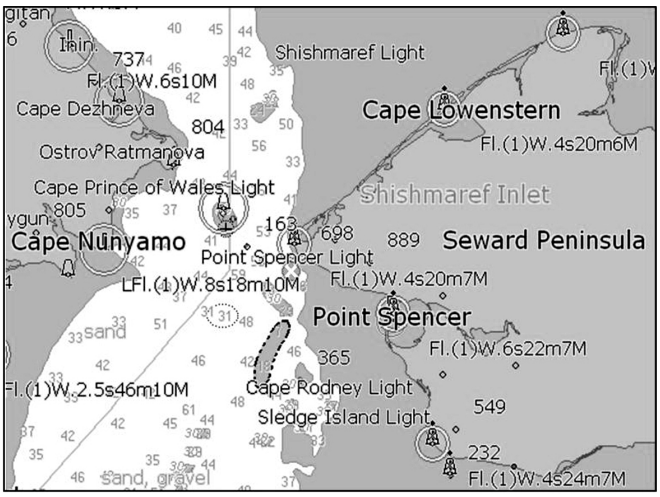


Figure 2: Sample eChart. (Ship Technology Global 2014)

1 An Integrated Bridge System is a combination of systems which are interconnected in order to allow centralized access to sensor information and command/control from workstations with the aim of increasing safe and efficient ship's management by suitably qualified personnel (International Maritime Organization 2016).

Several other satellite-based PNT systems are also in operation. In 1995, the same year that GPS became operational, the Russian Federation announced deployment of GLONASS. This system has been hampered by uneven funding and suffered a well-publicized 11-hour service outage in April 2014, among other failures. In May of 2016, a GLONASS expert provided a presentation on the details of this outage at the GNSS Conference in Croatia. In Asia, China has deployed its COMPASS (also known as Bei Dou) satellite navigation system. The system currently provides only regional coverage, however China has announced plans to provide global coverage by the year 2020. In Europe, the European Space Agency continues development of the GALILEO satellite navigation system. When complete, GALILEO will provide low-precision PNT services to the general public, while high-precision services will be available for a fee to commercial and military subscribers.

GNSS Signals

Signals produced by PNT satellite systems range between 1162 and 1610 MHz. Figure 3 depicts Lower and Upper L-Band frequency distribution of the four major GNSS. U.S. GPS emits two types of signals: (1) a Course Acquisition Code (referred to as the C/A code), which is broadcast on a single frequency and available free to all users; and (2) a second signal (referred to as the P(Y) code), which is broadcast on a separate encrypted frequency available only to the military. These two signals, C/A and P(Y) are equally accurate. However, the availability of the second signal on a different frequency allows the military to compensate for naturally occurring interference within the ionosphere, resulting in a more accurate fix and greater system resiliency.

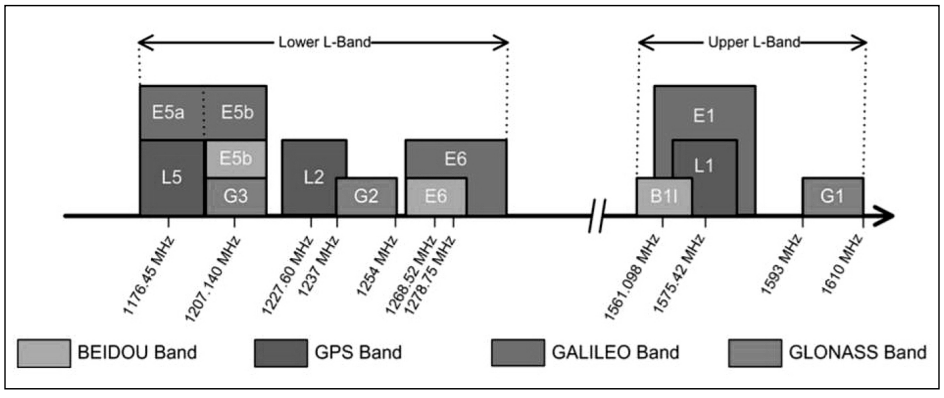


Figure 3: GNSS frequency bands, including all four global systems for 2017. (image courtesy of ExploreLabs.com 2015 at http://www.explorelabs.com/blog/designing-a-gps-receiver/)

It is important to note that GNSS pulses are extremely weak. GPS signals

have been compared with the light emitted by a "40 Watt light bulb as seen from 11,000 miles away (17,700 km)."[2] As such GNSS signals are vulnerable to:

1) *Jamming and Interference*. The broadcast of a stronger signal that intentionally or unintentionally blocks or impacts a GNSS satellite signal.

2) S*poofing*. The broadcast of a false GNSS signal, but at a slightly greater power. This deceives the GNSS receiver into locking onto the spoofed signal. Once the receiver has locked onto the stronger spoofed signal, the false signal gradually phases out of sync with the actual GNSS signal, causing the receiver to report false PNT data (information generated by the spoofer). This incremental phase out makes a spoofing attack very difficult to detect (The Mitre Corporation, 2014).

3) *Meaconing*. The intentional delay and rebroadcast of a GNSS signal intended to introduce error to receivers.

4) *Extreme Space Weather (ESW)*. Solar activity such as solar flares, coronal mass ejections, high-speed solar wind, and the impact of energetic particles on the earth's ionosphere.

5) *Other Vulnerabilities*. Kinetic or laser attacks to the satellite constellations or collisions with space debris are a few of other known susceptibilities of GNSS.

Shipboard Systems Affected by the Loss of GNSS Signals

A significant proportion of navigation equipment on the bridge of a modern ocean-going commercial vessel or offshore energy platform will likely be affected by the loss of GNSS signals. Various shipboard equipment and maritime aids which might suffer impacts are identified in Figure 4.

For components listed in Figure 4, the loss of GNSS may not prevent the component from functioning through an alternate sensor input. However, tests conducted by the General Lighthouse Authorities (GLA) of the United Kingdom and Ireland in 2008 showed how easily error messages and auditory warnings prompted by the loss of GPS can easily distract (and overwhelm) a vessel's bridge team (Grant et al. 2008). This can be especially dangerous for vessels operating in confined waterways, near shallow areas, or maneuvering in higher traffic densities.

2 Daniels, Charlie. 2014. Senior National Policy Analyst with Overlook Systems Technologies. (W. G. Kaag, Interviewer)

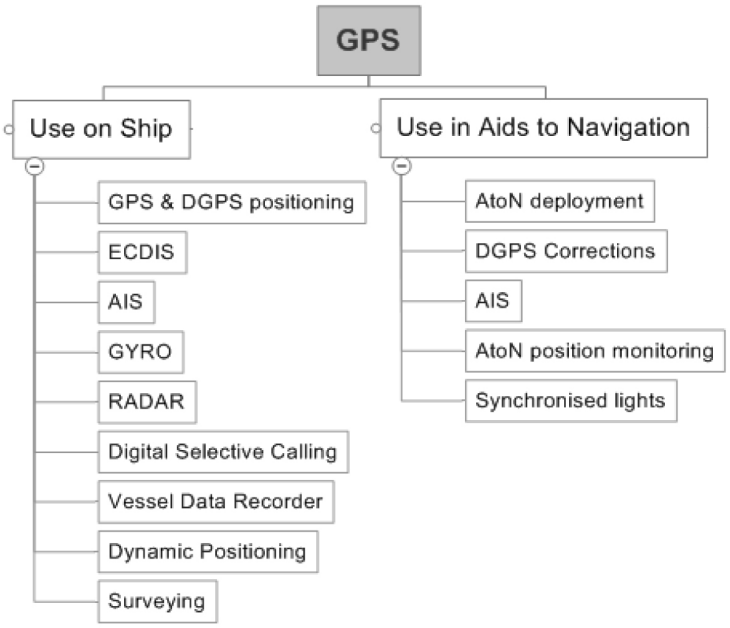


Figure 4: Maritime navigation equipment that uses GPS as a data input. (Grant et al. 2008)

These vulnerabilities are not unique to the maritime industry. A number of other industries are also at risk. For instance, the aviation and financial industries are heavily dependent on properly functioning PNT systems and would be affected in varying degrees by a cyber attack on GNSS. However, largely unique to the maritime industry is that much of marine environment information transfer is via radio frequency (RF) and not a dedicated hard-line network or directional microwave dish. A good example of this type of transfer is positioning by satellite systems. Data being sent to and from shipboard computers along with other shipboard technology is cyber; therefore, interference with the data flow constitutes a cyber threat.

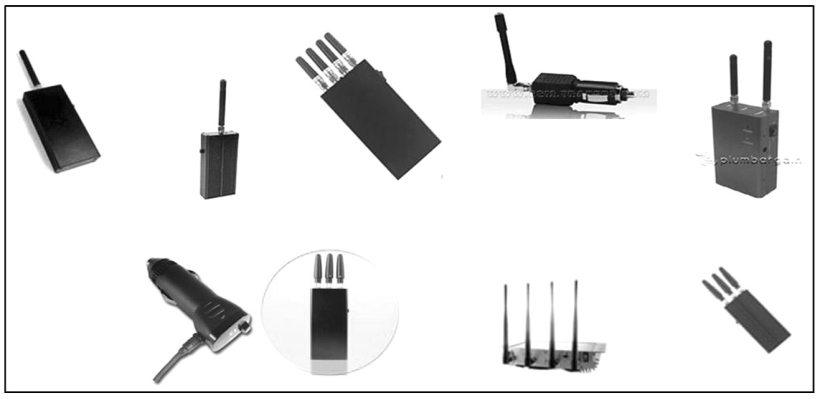


Figure 5: Small jammers that can be purchased via the Internet. Source: U.S. Government

GNSS Jamming Equipment

With some exceptions, use of GNSS jammers is generally illegal in the U.S., Canada and Europe. Despite this, jammers of various sizes and power ratings as illustrated in Figure 5 can be purchased via the internet. These small handheld jammers are extremely difficult for law enforcement officials to locate and suppress because they can be used intermittently, disguised or hidden easily, are highly mobile, and if necessary disposed of quickly by perpetrators.

As discussed by Jones in 2011, advanced GPS receivers are more resistant to jamming than conventional designs. Receivers equipped with nulling antennas[3] are more resistant to jamming than receivers without them (Jones 2011). In Figure 6, the purple dashed horizontal line indicates receiver tolerance for obtaining the coarse acquisition (C/A) code.

As described earlier, the course/acquisition (C/A) code is the worldwide PNT signal recognized by all civilian GPS receivers; a civilian GPS receiver must first acquire (or capture) and track the C/A signal to obtain navigational coordinates. A typical GPS receiver can successfully acquire and remain locked onto the C/A signal as long as the jamming environment is below the C/A code acquisition threshold of 27 dB for 100 km. Equally important, a minimal 1-Watt interference signal at a range of 100 km can prevent a typical C/A receiver from acquiring the GPS signal (Jones 2011).

[Michael Jones, 2011]:
"Theoretically, at least, a 10-milliwatt jammer will prevent a receiver from acquiring the C/A code at a distance of 10 kilometers, and a receiver already tracking the C/A code will lose lock about a kilometer from the jammer."

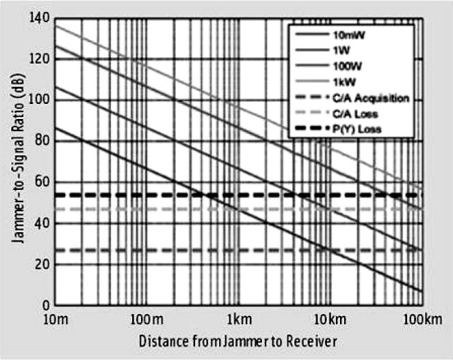


Figure 6: GPS jamming environment as a function of interference power and distance from jammer to the GPS receiver. The environment is given for four levels of interference power from 10 mW to 1kW (Jones 2011)

Figure 7 shows the area affected by a GPS jammer during tests conducted at Bridlington, U.K. along the coast of the North Sea in 2008. During the test, a jamming unit was positioned 25 m above ground level with a maximum power of 1.58 W. These tests demonstrated that relatively small jamming units can

3 "Nulling is a technique to reduce unwanted interference by selecting specifically against some characteristic of the interference" (LeComte, Henion and Schultz 1994).

affect GNSS reception over great distances (Grant et al. 2008).

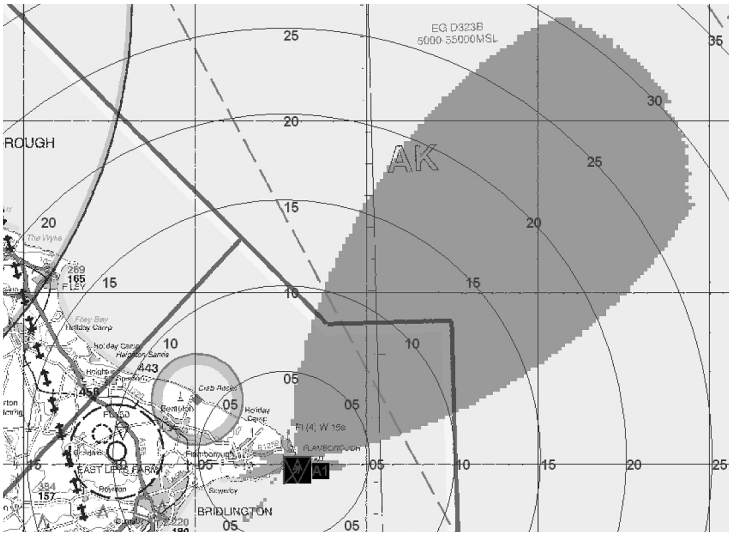


Figure 7: Coverage area of the GPS jamming unit at 25 m above ground level on maximum power of 1.58 W ERP. (Grant et al. 2008—Image courtesy of DSTL), ranges in km

Threat Scenarios

At this time, the most likely GPS maritime threat scenarios to consider include:

Jamming of a port or other congested waterway by an individual or small group of non-state actors using small, portable jammers. Rapid movement of these individuals, coupled with intermittent use of the jammer(s) would make it very difficult for local law enforcement officials to track and arrest the perpetrators quickly. Attacks of this type can lead to significant economic losses as well as loss of confidence by system users.

State-sponsored GNSS Jamming. The most well-documented examples of state sponsored jamming attacks occur in the Republic of Korea (Seo and Kim 2013). The findings of Seo and Kim by attack date, jammer location, affected area and disruption are summarized in Figure 8–Table 1. On three different occasions, the Republic of Korea was subjected to intentional, high-power jamming by North Korea over a wide area. The sources of these attacks appear to have been large truck-mounted jamming units placed at strategic geographic locations. Amongst the many attacks that have been conducted, the 2012 attack affected over 1,000 aircraft and 250 ships (Seo and Kim 2013).

By June of 2016, United Press International (UPI.com) reported that North Korea had sent over 2100 jamming signals to the south since January resulting in widespread interference and disruptions to South Korea (Shim 2016).

Intentional High-Power Jamming of Republic of Korea			
Dates	August 23–_26, 2010	March 4–_14, 2011	August 28—May 13, 2012
Jammer Locations	Kaesong	Kaesong and Mt. Kumgang	Kaesong
Affected Areas	Gimpo, Paju, Gangwon	Gimpo, Paju, Gangwon	Gimpo, Paju, Gangwon
GPS Disruptions	181 cell towers, 15 aircraft, 1 military vessel	145 cell towers, 106 aircraft, 10 vessels	1,016 aircraft, 254 vessels

Table 1: Source: (Seo and Kim 2013)

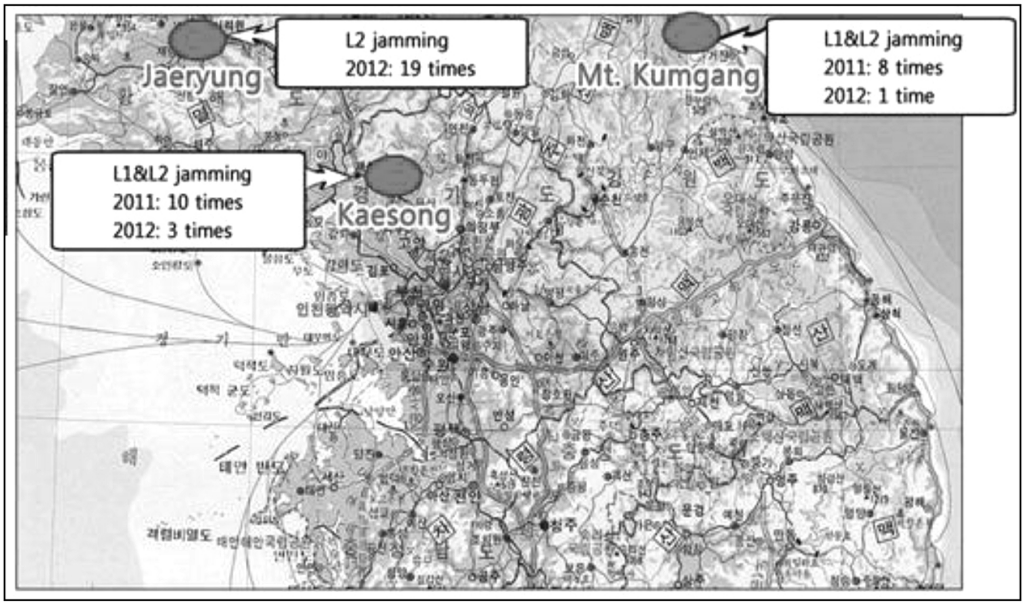


Figure 8: Location of North Korean Jammers. (Seo and Kim 2013)

*State-sponsored Spoofing***.** Eventually, spoofing may pose a significant maritime threat to GNSS as it has the potential to lead vessels astray into dangerous waters, resulting in significant loss of life (cruise liners and ferries) or environmental damage. Presently, spoofing requires a level of technical sophistication that is normally presented through nation states. However, small groups have conducted successful spoofing tests, most notably students at the University of Texas under Professor Todd Humphreys.[4]

Primary Defenses Against Jamming

Improved Maritime Training and Education. One of the most cost-effective counter measures to defend against the intentional or unintentional jamming of GNSS signals is crew training. If trained and educated properly, commercial

4 University of Texas spoofing tests are viewable on YouTube, "Spoofing on the High Seas." http://www.youtube.com/watch?v=ctw9ECgJ8L0#t=38.

ship crews should be capable of operating their vessels in GNSS compromised environments. Ship crews should be taught how GNSS systems interact with ship systems and how to recognize when GNSS signals may have been compromised. The maritime industry should also be encouraged to maintain basic seamanship skills, such as dead reckoning and the ability to use piloting instruments. Routine ship drills should include signal loss and spoofing of the signal.

*Improved Equipment***.** Development continues on new GPS receivers that can identify non-GPS signals by their relative location (jamming and spoofing signals come from the terrestrial locations not satellites) and their strength (jamming and spoofing signals must by necessity be stronger than GPS satellite-generated signals). In addition to receiver signal strength alarms and specialized antennas, the effects of intentional jamming could be mitigated through the use of inertial navigation systems (INS) and radio frequency (RF) jamming detectors. However, at this point in time it is unclear when such equipment would be available to and employed by the commercial industry, or how much it will cost.

Installation of Powerful Alternate Ground Based PNT Systems. Coastal nations most at risk should consider the installation of alternate (back-up) or complementary, land-based PNT systems, such as enhanced LORAN (known as eLoran). Both the United Kingdom and the Republic of Korea are in the process of installing eLoran systems. Seo and Kim reported that the Republic of Korea initially proposed five locations for eLoran transmitters as shown in Figure 9. The benefit of such systems is to provide PNT users with a more resilient PNT signal—one that is too powerful to be effectively jammed or spoofed. Also the low frequency of the powerful terrestrial eLoran signals permits PNT reception in GNSS denied environments. Examples include indoor structures (especially heavy buildings), underground in parking garages and basements, underwater, urban canyons, and dense foliage.

Conclusions

Worldwide dependence on Global Navigation Satellite Systems (GNSS) continues to grow. Ongoing advancements in jamming technology and the availability of small, portable jammers constitute a significant threat to maritime commerce and safety. In the face of a GNSS jamming attack, most commercial ports could be forced to suspend operations until the source of the interference is located and suppressed. It is very possible that a group of individuals operating small, portable jammers could force the closure of a major seaport or international maritime chokepoint. The economic consequences of such an attack could run into the billions of dollars.

In the long-term we also anticipate that more powerful jamming technolo-

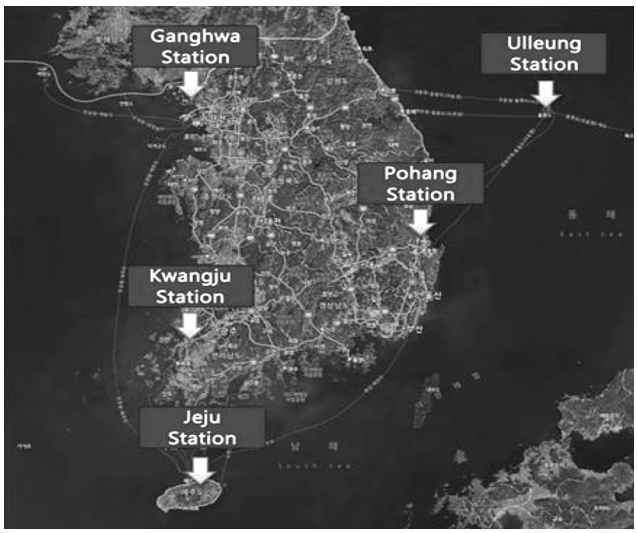


Figure 9: Location of proposed South Korean eLoran transmitters (Seo and Kim 2013)

gy and delivery systems (such as broadband jammers and drones) will become widely available and constitute two of the greatest threats to GNSS. The maritime community needs to become more vigilant, actively train to recognize and respond to both jamming and spoofing attacks, and encourage the immediate installation of complementary PNT systems such as eLoran for strategic maritime locations.

Research Tips

1. For over half a century, Loran A and Loran C provided an alternate means of positioning independent of GNSS fixing, celestial, radar or terrestrial piloting when in or near U.S. waters. In 2010 when the USCG halted its Loran C transmissions, GNSS/GPS became the de facto sole source for nearly all position fixing. For several decades, in U.S. offshore environments, Loran C had provided a confirmation of GNSS positioning that was considered critical by the USCG, NTSB and other entities concerned with vessel safety. Consider researching investigation results for groundings like the M/V ROYAL MAJESTY as far back as 1995 (Grounding of the Panamanian Passenger Ship Royal Majesty). Keywords include Loran C, Chayka, sole-source positioning, Terrestrial PNT, GPS and GNSS Vulnerabilities.

2. NAVSTAR (U.S. GPS) information including signals, infrastructure and future is provided in great detail at http://www.gps.gov/. Improvements to GPS security through upgrades in satellites, ground networks and receivers are presented. Another important U.S. site for GPS/NAVSTAR information

is the U.S. Coast Guard Navigation Center at http://www.navcen.uscg.gov/?pageName=gpsmain.

3. GNSS jamming and spoofing incidents are seldom reported as users are often unaware their receiver is experiencing interference receiving the satellite signals. Whether the interference is unintentional or purposeful, the impacts to an unwary navigator may be quite serious. Keywords to consider here are GPS/GNSS jamming, GPS/GNSS spoofing, GPS/GNSS meaconing, ECDIS, eCharts, precise positioning. Search out jamming reports such as the incident referred to in the USCG Marine Safety Alert at http://www.uscg.mil/hq/cg5/cg545/alerts/0116.pdf. The U.S. DoD's Purposeful Interference Response Team (PIRT) has been instrumental in promoting recognition and reporting of interference incidents worldwide.

4. Both GPS and GLONASS GNSS have suffered serious failures in the recent past where position fixing and/or precision timing became compromised for a large segment of users. Consider reviewing the two most recent events: GPS on January 26, 2016 and GLONASS on April 1, 2014 to gain perspective on the serious consequences that can develop.

5. eLoran Systems and eLoran Studies are searchable in, for example, private trade publications and government sites covering GNSS PNT. For instance, the DHS S&T website is reporting on precision timing by eLoran in releases like DHS S&T Demonstrates Precision Timing ... —Homeland Security which may also be sited on corporate websites like DHS and UrsaNav Successfully Demonstrate Timing Inside NYSE ... Another governmental (United Kingdom and Ireland) site that has much information on eLoran is at the General Lighthouse Authority: http://www.gla-rrnav.org/

6. Emerging technologies pose constant security challenges for all sectors including Maritime Transportation. GNSS sole-source issues continue to be a concern for other reasons as, for instance, drone technology expands. Drones can easily carry jammers and increase their efficiency by raising the jamming signal altitude and other reasons. Another looming technology, autonomous ships, will need to rely as never before on electronic positioning and specifically GNSS fixing. As the sole-source available with no navigator onboard, GNSS signals and positioning will need to leave no room for error. Consider: "The prudent navigator will not rely solely on any single aid to navigation." (USCG Notices to Mariners)

References

Aristova, Victoria. 2016. "GLONASS." 10th Annual Baška GNSS Conference, Croatia. Sponsored by Royal Institute of Navigation, University of Zagreb and University of Rijeka.

Grant, Allen, Paul Williams, Nick Ward, and Sally Basker. 2008. "GPS Jamming and the Impact on Maritime Navigation." http://www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf.

International Maritime Organization. 2016. "Integrated Bridge System (IBS)." http://www.imo.org/en/OurWork/Safety/SafetyTopics/Pages/IntegratedBridgeSystems.aspx.

Jones, Michael. 2011. "The Civilian Battlefield: Protecting GNSS Receivers from Interference and Jamming." *Inside GNSS.* http://www.insidegnss.com/auto/marapr11-Jones.pdf.

Last, David. 2016. "GNSS/PNT/eLoran." 10th Annual Baška GNSS Conference, Croatia. Sponsored by Royal Institute of Navigation, University of Zagreb and University of Rijeka.

LeComte, Wiliam, Scott R. Henion, and Peter A. Schultz. 1994. "Adaptive Wideband Optical Nulling for an Antenna System." Proc. SPIR 2155, Optoelectronic Signal Processing for Phased-Array Antennas IV, 256.

Moskoff, David. 2014. "GPS Jammers a Top Concern in Maritime Cyber Readiness." *Professional Mariner.* http://www.professionalmariner.com/June-July-2014/GPS-jammers/.

"National Coordination Office for Space-Based Positioning, Navigation, and Timing." 2014. www.gps.gov.

Ruddock, Alan. 2013. "Sports Equipment: Is GPS the Best Route to Performance Analysis?" *Peak Performance Lite.* www.pponline.co.uk.

Seo, Jiwon, and Mincheol Kim. 2013. "eLoran in Korea – Current Status and Future Plans." http://www.govexec.com/media/gbc/docs/pdfs_edit/061813bb2.pdf.

Shim, Elizabeth. 2016. "North Korea sent 2100 GPS Jamming signals to South."UPI.com.http://www.upi.com/Top_News/World-News/2016/06/29/North-Korea-sent-2100-GPS-jamming-signals-to-South/8211467212439/.

"Ship Technology Global." 2014. www.ship-technology.com.

The Mitre Corporation. 2014. www.mitre.org.

University of Texas at Austin. 2014. "Professor Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV." *Aerospace Engineering and Engineering Mechanics*. http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing.

USCG Marine Safety Alert 01-16. 2016. "Global Navigation Satellite Systems—Trust, But Verify, Report Disruptions Immediately." USCG Inspections & Compliance Directorate. http://www.uscg.mil/hq/cg5/cg545/alerts/0116.pdf.

U.S. Department of Homeland Security. 2016. "DHS S&T Demonstrates Precision Timing Technology at New York Stock Exchange." DHS Science & Technology Press Release. https://www.dhs.gov/science-and-technology/news/2016/04/20/st-demonstrates-precision-timing-technology-ny-stock-exchange.